REMARKS

Claims 1 to 42 were pending in the Application at the time of examination. The Examiner objected to Claims 11, 22 and 33 for failing to spell out JXTA. The Examiner rejected Claims 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36 37, 38, 39, 40, 41, and 42 under 35 U.S.C. 103(a) as obvious over the Vigue et al. reference (US 2003/0163702A1) in view of the Winget et al. reference (US2005/0120213A1). The Examiner rejected Claims 5, 11, 16, 22, 27 and 33 under 35 U.S.C. 103(a) as obvious over the Vigue et al. reference (US 2003/0163702A1) in view of the Winget et al. reference (US2005/0120213A1) and further in view of the Rutherglen et al. reference (US2003/0033517A1).

Applicants have amended Claims 35, 36, 41 and 42 to correct informalities. Claims 1 to 42 remain in the Application.

OBJECTION TO CLAIMS 11, 22 AND 33

The Examiner objected to Claims 11, 22 and 33 for failing to spell out JXTA.

Applicants respectfully submit that JXTA is not an acronym, as the Examiner apparently believes, but is rather a project, and architecture name/trademark, well known in the art. The name is short for Juxtapose, as in side by side, but is not an acronym or proper abbreviation. It is recognition that peer to peer is juxtaposed to client server or Web based computing, what is considered today's traditional computing model.

This fact can be established by checking the website at http://wiki.java.net/bin/view/Jxta/JxtaFaqGeneral#What does JXTA stand for

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Since JXTA is not an acronym, Applicants respectfully submit that there is no "spelling out" to be done. Consequently, Applicants respectfully request the Examiner withdraw the rejection of Claims 11, 22 and 33.

REJECTION OF CLAIMS 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36 37, 38, 39, 40, 41, AND 42 UNDER 35 U.S.C. 103(a)

The Examiner rejected Claims 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36 37, 38, 39, 40, 41, and 42 under 35 U.S.C. 103(a) as obvious over the Vigue et al. reference (US 2003/0163702A1) in view of the Winget et al. reference (US2005/0120213A1).

Applicants' independent Claim 1, reads as follows, with emphasis added:

A method for securing a communication between a peer node and **an intermediary peer node** in a peer-to-peer network, the method comprising:

the peer node generating a secured communication request to the **intermediary peer node**;

the **intermediary peer node** **authenticating the peer node in response to said secured communication request**, and

the **intermediary peer node** issuing a signed certificate of authority upon successful authentication.

Applicants' independent Claim 12, reads as follows, with emphasis added:

A method for securing a communication between a peer node and an **intermediary peer node** in a peer-to-peer network, the method comprising:

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

generating a secured communication request to the **intermediary peer node capable of authenticating the peer node in response to said secured communication request**, and

receiving a signed certificate of authority upon successful authentication.

Applicants' independent Claim 23, reads as follows, with emphasis added:

A method for securing a communication between a peer node and an **intermediary peer node** in a peer-to-peer network, the method comprising:

receiving a secured communication request from the peer node;

authenticating the peer node in response to said secured communication request; and

sending a singed certificate of authority upon successful authentication.

Applicants' independent Claim 34, reads as follows, with emphasis added:

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for securing a communication between a peer node and an **intermediary peer node** in a peer-to-peer network, the method including:

the peer node generating a secured communication request to the **intermediary peer node**;

the **intermediary peer node** **authenticating the peer node in response to said secured communication request**, and

the **intermediary peer node** issuing a signed certificate of authority upon successful authentication.

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Applicants' independent Claim 35, as amended, reads as follows, with emphasis added:

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to-peer networks, the method including:

generating a secured communication request to an **intermediary peer node** capable of authenticating the peer node in response to said secured communication request, and

receiving a signed certificate of authority upon successful authentication.

Applicants' independent Claim 36, as amended, reads as follows, with emphasis added:

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to-peer networks, the method including:

an intermediary peer node receiving a secured communication request from a peer node;

authenticating the peer node in response to said secured communication request; and

sending a signed certificate of authority upon successful authentication.

Applicants' independent Claim 37 reads as follows, with emphasis added:

An apparatus for securing a communication between a peer node and **an intermediary peer node** in a peer-to-peer network comprising:

means for generating a secured communication request to the **intermediary peer node**;

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

means **for authenticating the peer node** in response to said secured communication request, and

means for issuing a signed certificate of authority upon successful authentication.

Applicants' independent Claim 38 reads as follows, with emphasis added:

An apparatus for securing a communication between a peer node and **an intermediary peer node** in a peer-to-peer network comprising:

means for generating a secured communication request to the **intermediary peer node capable of authenticating the peer node in response to said secured communication request**, and

means for receiving a signed certificate of authority upon successful authentication.

Applicants' independent Claim 39 reads as follows, with emphasis added:

An apparatus for securing a communication between a peer node and **an intermediary peer node** in a peer-to-peer network comprising:

means for receiving **a secured communication request from the peer node**;

means for authenticating the peer node in response to said secured communication request; and

means for sending a signed certificate of authority upon successful authentication.

Applicants' independent Claim 40 reads as follows, with emphasis added:

A peer-to-peer network system comprising:

a peer node;

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

an **intermediary peer node communicatively coupled to said peer node;**

wherein said peer node is **configured to generate a secured communication request to said intermediary peer node;**

wherein said **intermediary peer node** is **configured to authenticate said peer node in response to said secured communication request,** and

wherein said **intermediary peer node** is configured to issue a signed certificate of authority upon successful authentication.

Applicants' independent Claim 41, as amended, reads as follows, with emphasis added:

A peer node comprising:

a processor; and

a memory comprising program instructions, wherein the program instructions are executable by the processor to:

generate a secured communication request to **an intermediary peer node capable of authenticating the peer node in response to said secured communication request,** and

receive a signed certificate of authority upon successful authentication.

Applicants' independent Claim 42, as amended, reads as follows, with emphasis added:

An **intermediary peer** node comprising:

a processor; and

a memory comprising program instructions, wherein the program instructions are executable by the processor to:

receive a secured communication request from a peer node;

authenticate the peer node in response to said secured communication request; and

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

send a signed certificate of authority upon successful authentication.

As shown above each of Applicants' independent Claims recites both an intermediary peer node and authentication of a peer node by the intermediary peer node.

An intermediary peer node, also called a "super peer" or "super peer node", is defined in Applicants' Specification at, for example, page 8, paragraph [0014] to page 9, paragraph [0016], which reads as follows, with emphasis added:

Super peer nodes are peer nodes that serve as an intermediary contact point for administrative information that concerns the super peer nodes as well as the subset of the P2P network of which they are aware and for which they are responsible. These super peer nodes may be used to respond to Certificate Service Requests from peer nodes.

FIG. 2 is a diagram schematically illustrating intermediary peer nodes mediated P2P connections in accordance with one embodiment of the present invention. To improve peer node discovery, responsiveness of communication, and routing super-peers have been introduced into P2P network topologies. A first peer node 202 is connected to a network connection 204, such as the internet, through a first Network Address Translator (NAT) 206. **A first super peer node 208 is connected to the network connection 204 through a first JXTA relay 209 and a first router 210. A second super peer node 212 is connected to the network connection 204 through a second JXTA relay 213 and a second router 214. A second peer node 216 is connected to the network connection 204 through a second Network Address Translator (NAT) 218.** It must be understood that there may be multiple routers in these network paths as well as firewalls. FIG. 2 is illustrative of one of many means to separate peer nodes and super peers on the Internet.

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Super peers, **also known as intermediary peer nodes**, may be added with a minimal amount of centralization, and may be placed in an ad-hoc topology to be discovered by chance, or by an email message containing a known IP address and a port of a super peer. Once the presence of the super peer is known, the knowledge of their existence can be propagated amongst the peer nodes or edge-peers as they contact one another. Such super peers 208, 212, may also serve as a contact point for administrative information that concerns the super peers themselves as well as the subset of the P2P network (in FIG. 2, the subset of the P2P network includes peer node 202 and peer node 216) of which they are aware and for which they are responsible.

As shown above, in accordance with Applicants' Specification, an "intermediary peer node" is defined specifically as a "Super Peer Node" with specific properties, not simply another node on the P2P network.

In addition, at paragraphs [0017] to [0021] of Applicants' Specification, Applicants specifically state, with emphasis added, that:

With respect to the implementation of securing P2P networks, the present invention is described in the context of ad-hoc JXTA P2P networks. The present description is for illustrative purposes and **the method for securing P2P networks is independent of the implementation of the underlying P2P platform as long as this platform adheres to the following minimal characteristics**:

1. **The P2P network topology is organized around super peers** such as super peer node 208 and super peer node 212 in FIG. 2.

2. **The super peer nodes have knowledge of one another, and have the ability to communicate with one another on the P2P network.**

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

In FIG. 2, super peer node 208 is aware of the existence of super peer node 212 and super peer node 208 can communicate with super peer node 212 via routers 210, 214 and network connection 204.

3. **Each peer node of the P2P network connects to at least one of the super-peers on a regular basis**. For example, peer nodes 202 and 216 connect to super peer node 212 on a regular basis.

One of the primary axioms of P2P networks is end-to-end communication: any two peer nodes must be able to communicate, and either of them must be able to initiate a connection to the other. Because peer nodes 202, 216 are both NAT bound, neither peer nodes 202 and 216 can initiate connections to one another unless a connection is mediated through a common known third party intermediary, such as super peer node 212. In FIG. 2, peer node 202 communicates with peer node 216 via super peer node 212. Discovery or address lookup given a name is therefore handled by the super peers 208 and 212. The same initiation of communication barrier can be affected by a firewall or combinations of NAT and firewalls.

As shown above, in accordance with Applicants' Specification, an intermediary peer node is defined specifically as a "Super Peer Node" with specific properties, not simply another node on the P2P network, and the intermediary peer nodes, as defined, are required.

However, in making the rejection of Claims 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 15, 17, 18, 19, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36 37, 38, 39, 40, 41, and 42, the Examiner states that the Vigue reference discloses "the peer node generating a secured communication request to the **intermediary peer node"** in Vigue's "Abstract of the Disclosure".

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

Vigue's "Abstract of the Disclosure" reads as follows, with emphasis added:

A system and method for secure and verified sharing of resources in a peer-to-peer network environment to facilitate efficient use of bandwidth are disclosed. The method for securely sharing resources over a peer-to-peer network generally comprises **broadcasting a request by a requesting peer** for a resource over the peer-to-peer network where the resource is identified with a resource version identifier, **receiving a response from a responding peer on the peer-to-peer network indicating that the responding peer has the requested resource**, retrieving the requested resource from the responding peer, and verifying the retrieved resource by ensuring the retrieved resource contains the version identifier embedded therein. Preferably, the verifying also includes verifying a digital signature, such as a 1024-bit VeriSign digital certificate, of the retrieved resource to ensure integrity of the retrieved resource.

Consequently, in making the rejection, the Examiner is equating an **intermediary peer node** as any responding peer on the P2P network that indicates it has access to a given resource. However, as discussed above, in accordance with Applicants' Specification, an intermediary node is defined specifically as a "Super Peer Node" with specific properties, not simply another node on the P2P network as the Examiner asserts. Indeed, nowhere in the Vigue reference, the Winget reference, or the Rutherglen reference are any of the terms intermediary, intermediary peer, intermediary peer node, super, super peer, or super peer node found, nor are any nodes having the defined properties of an intermediary peer node disclosed.

In light of the discussion above, Applicants respectfully submit that the Examiner has failed to show where in the Vigue reference, the Winget reference, or any proper combination of

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

the Vigue reference and the Winget reference, an intermediary peer node, as defined in Applicants' Specification, is described, disclosed, taught or suggested. Consequently, Applicants respectfully request the Examiner withdraw the rejection of Claims 1, 12, 23, 34, 35, 36, 37, 38, 39, 40, 41 and 42, as amended, and allow Claims 1, 12, 23, 34, 35, 36, 37, 38, 39, 40, 41 and 42 to issue.

In addition, Claims 2 to 11 depend, directly or indirectly, on Claim 1, Claims 13 to 22 depend, directly or indirectly, on Claim 12, and Claims 24 to 33 depend, directly or indirectly, on Claim 23. Consequently, Applicants respectfully request the Examiner withdraw the rejection of Claims 2 to 11, 13 to 22, and 24 to 33, and allow Claims 2 to 11, 13 to 22, and 24 to 33 to issue as well for at least the reasons discussed above.

REJECTION OF 5, 11, 16, 22, 27 and 33 UNDER 35 U.S.C. 103(a)

The Examiner rejected Claims 5, 11, 16, 22, 27 and 33 under 35 U.S.C. 103(a) as obvious over the Vigue et al. reference (US 2003/0163702A1) in view of the Winget et al. reference (US2005/0120213A1) and further in view of the Rutherglen et al. reference (US2003/0033517A1).

As discussed above, Applicants respectfully submit that the Examiner has failed to show where in the Vigue reference, the Winget reference, or any proper combination of the Vigue reference and the Winget reference, an intermediary peer node, as defined in Applicants' Specification, is described, disclosed, taught or suggested. Applicants further submit that the addition of the Rutherglen reference does nothing to cure this deficiency of the Vigue reference, the Winget reference, or any proper combination of the Vigue reference and the Winget references. Consequently, Applicants respectfully submit that the Examiner has failed to show where in the Vigue reference,

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888

the Winget reference, the Rutherglen reference, or any proper combination of the Vigue reference, the Winget reference, and the Rutherglen reference, an intermediary peer node, as defined in Applicants' Specification, is described, disclosed, taught or suggested.

Claims 5 and 11 depend on Claim 1. Claims 16 and 22 depend on Claim 23. Claims 27 and 33 depend on Claim 23. Consequently, Applicants respectfully request the Examiner withdraw the rejection of dependent Claims 5, 11, 16, 22, 27 and 33 and allow Claims 5, 11, 16, 22, 27 and 33 to issue for at least the reasons discussed above with respect to parent Claims 1, 12 and 23.

CONCLUSION

For the foregoing reasons, Applicants respectfully request allowance of all pending Claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicants.

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office via the Office's EFS-Web system on the date shown below.

Attorney for Applicants — October 17, 2008 Date of Signature

Respectfully submitted,

Philip McKay
Attorney for Applicants
Reg. No. 38,966
Tel.: (831) 655-0880

GUNNISON, McKAY & HODGSON, L.L.P.
Garden West Office Plaza
1900 Garden Road, Suite 220
Monterey, CA 93940
(831) 655-0880
Fax (831) 655-0888